REMARKS/ARGUMENTS

The Advisory Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Office Action.

Claim Rejections – 35 USC § 103

At page 3 of the Advisory Action, the Examiner rejects claims 1 to 6, 8, 9, 11 to 19, 21, 22, and 24 to 27 as being unpatentable over Shigenaga (US Patent No. 4,710,613) in view of Lee (US Patent No. 5,923,759.

Reconsideration and withdrawal of this rejection is respectfully requested in light of the following comments.

Obviousness can only be established by combining or modifying teachings of the prior art to produce the claimed invention where there is some teaching, suggestion or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

The Examiner states on page 5 that:

> *"Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67)"*

However, on closer inspection of the section of Lee which the Examiner has highlighted, in fact Lee describes two **separate routines that are performed separately**.

In particular, lines 37 to 53 describes the "Authenticate Card Routine 300" which is used for *"allow[ing] system 100 to determine whether a card inserted into one of the card units is authentic"* (Column 6, lines 37 to 40). The "Authenticate Card Routine 300" comprises the steps of:

- a processor 122 generating a random number (column 6, lines 40 and 41);

- processor 122 transmits generated random number to the card (column 6, line 41);
- card receives random number; (column 6, lines 41 to 42);
- card encrypts random number using algorithm and an "internal key" (column 6, lines 42 to 43);
- card returns encrypted random number to processor 122 (column 6, line 44);
- processor 122 decrypts the encrypted number based upon same algorithm and an identifying key (column 6, lines 46 to 48); and
- processor 122 compares the original random number to the decrypted random number to determine authenticity of the card (column 6, lines 48 to 50).

It is important to note that the "Authenticate Card Routine 300", used for authenticating the card, fails to describe the card decrypting any data.

In a totally separate routine as shown in Figure 3, Lee describes at column 6, lines 53 to 65 the "Authenticate Host Routine 310" which is used *"to allow a card to determine whether the processing system in which the card is inserted is authentic"*. Thus, Lee describes that this routine is used by the card to determine the authenticity of the host.

Therefore "Authenticate Card Routine 300" is in total contrast to "Authenticate Host Routine 310" because "Authenticate Card Routine 300" is used for authenticating the card whereas "Authenticate Host Routine 310" is used for authenticating the host. Nowhere in Lee is it suggested that these two routines could be combined to only authenticate the card.

Furthermore, the "Authenticate Host Routine 310" is in total contrast to claim 1 which requires *"validating the authenticity **of the untrusted authentication chip contained within a consumable**"*. Claim 1 is not used for determining the authenticity of the trusted authenticated chip which may be a printer or the like. Claim 1 is directly related to claiming a method of authenticating the authentication chip within the consumable.

Thus, lines 53 to 65 of column 6 which the Examiner has highlighted are irrelevant to the claims. The claims are not directed to authenticating the trusted authentication chip as by virtue the trusted authentication chip is already trusted and authenticated.

Accordingly, the combined teachings of lines 37 to 40 in column 6 of Lee and the disclosure of Shigenaga fail to teach or suggest decrypting the received data in the consumable with a second secret key and also encrypting data using the same second secret key. Furthermore, the combined teachings of Shigenaga and lines 37 to 40 in column 6 of Lee fail to teach or suggest encrypting and decrypting in the trusted authentication chip with the same first key.

Shigenaga actually teaches the very opposite to the claimed method. At lines 53 to 58 Shigenaga states:

> *"According to the encryption system based on the RSA algorithm,* ***the data encrypted by the 'PUK' is fairly hard to be decrypted by the same 'PUK' but can be decrypted only by the 'PRK'****..."*

In light of this highlighted section in Shigenaga, a person skilled in the art would conclude that the key used to encrypt the data in the processor 122 can only be used for encrypting data and that a separate key must be used for decrypting. Therefore, a person skilled in the art would not be motivated to use the key used for encryption also for decrypting received encrypted data, as Shigenaga teaches that there would not be a reasonable expectation of success.

The MPEP states at 2143 "*Basic Requirements of a Prima Facie Case of Obviousness*" that:

> "... *three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.*
>
> *The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*"

Thus as Shigenaga and Lee fail to teach or suggest the limitations of:

- authenticating the consumable by encrypting and decrypting data in the trusted authentication chip using the same first key; and,
- authenticating the consumable by encrypting and decrypting data in the consumable using the same second private key;

and as Shigenaga teaches that there would be no reasonable expectation of success, the applicant submits that independent claims 1 and 14 are patentable over Shigenaga in view of Lee as required by MPEP at 2143.

The applicant respectfully requests that Examiner withdraw the rejection to all the claims.

In any event, the Applicant respectfully submits that a skilled person in the art would not be motivated to combine Shigenaga with Lee as the cited documents teach very opposing authentication systems.

Shigenaga discloses:

- Card terminal generating a random number and encrypts twice;
- Card terminal sending encrypted data to card IC;
- Card IC decrypting the encrypted data and determines the random number;
- Card IC sending determined random number back to card terminal; and,
- Card terminal comparing both the time of processing, and the original and received random numbers to determine authenticity.

Thus, when one compares Shigenaga with the "Authenticate Card Routine 300" disclosed in Lee which was previously discussed, it is apparent that the cited documents are totally different. For example:

- Shigenaga teaches encrypting the random number prior to sending to card, whereas in contrast to Lee which teaches sending the random number unencrypted;
- Shigenaga teaches decrypting in the card IC, whereas in contrast Lee fails to teach decrypting in the card IC to authenticate the card;
- Shigenaga teaches sending the random number back to the terminal in unencrypted form, whereas in contrast Lee teaches sending the random number to the host in encrypted form; and,
- Shigenaga teaches that the terminal compares the received data to the stored random number, whereas in contrast Lee teaches that the data needs to be unencrypted prior to comparison.

Therefore, with such a large number of contrasting features of the respective systems, the applicant submits that a skilled person in the art would simply not be motivated to combine Shigenaga with Lee.

Furthermore, Shigenaga suggests that it is essential that the authentication is performed by comparing the actual processing time with the estimation processing time. Lee fails to suggest any such feature. Therefore, it is submitted that a person skilled in the art would simply not be motivated to combine Shigenaga which relies on comparing processing times with Lee which simply compares random numbers.

Additionally, a skilled person in the art would not be motivated to combine Shigenaga with Lee since both are directed to encrypting and decrypting random numbers at totally opposite ends of the system (ie. at the host or at the card).

As required under MPEP at 2143, "*...there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.*" There is no suggestion or motivation in either Lee or Shigenaga that two opposing authentication techniques could be combined since there is a large number of contrasting features. Additionally, there is no suggestion or motivation in the knowledge generally available to one of ordinary skill in the art that a public key used for encrypting could also be used for decrypting data for authenticating an untrusted authentication chip. Furthermore, there is no suggestion or motivation in the knowledge generally available to one of ordinary skill in the art that a private key used for decrypting could also be used for encrypting data for authenticating an untrusted authentication chip.

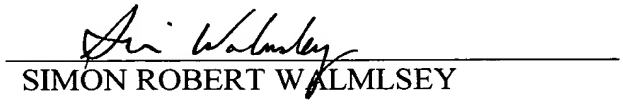
Therefore, there is no motivation to combine Shigenaga with Lee for authenticating an untrusted authentication chip in a consumable. Thus, as required under MPEP at 2143, all the claims are patentable. Reconsideration and withdrawal of the rejection is respectfully requested.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 U.S.C. §103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:



SIMON ROBERT WALMLSEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762